**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

June 10, 2016

*The following cyber advisory was issued by the State of Alaska and
was intended for State government entities. The information may or
may not be applicable to the general public and accordingly, the State
does not warrant its use for any specific purposes.*

ADVISORY NUMBER:
SA2016-089

DATE(S) ISSUED:
06/07/2016

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been identified in Mozilla Firefox and Firefox ESR, which
could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access
the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed
in large organizations. Exploitation of these vulnerabilities could allow an attacker to
bypass same-origin policy restrictions to access data, and execute arbitrary code in the
context of the affected application.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Mozilla Firefox versions prior to 47
- Mozilla Firefox ESR versions prior to 45.2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Mozilla has confirmed multiple vulnerabilities in Firefox and Firefox ESR. Exploitation of these vulnerabilities could allow for arbitrary code execution, bypass the same-origin policy and other security restrictions, and perform unauthorized actions. These vulnerabilities could be exploited if a user visits or is redirected to a specially-crafted webpage or opens a specially-crafted file. Details of these vulnerabilities are as follows:

- Multiple memory corruption vulnerabilities that could allow remote code execution. (CVE-2016-2815)
- A buffer overflow vulnerability when parsing HTML5 fragments in a foreign context such as under an <svg> node. (CVE-2016-2819)
- A use-after-free vulnerability when deleting document object model (DOM) table elements created within the editor that could result in a exploitable crash. (CVE-2016-2821)
- An addressbar spoofing vulnerability that can be utilized to mask the true site URL allowing for spoofing by a malicious site. (CVE-2016-2822)
- An out-of-bounds vulnerability when using the ANGLE graphics library. (CVE-2016-2824)
- A partial same-origin-policy vulnerability through setting 'location.host' through data URI. (CVE-2016-2825)
- A file overwrite and privilege escalation vulnerability through Mozilla Windows Updater. (CVE-2016-2826)
- A Use-after-free vulnerability when textures are used in WebGL operations after recycle pool destruction. (CVE-2016-2828)
- A vulnerability when requesting permissions in short succession that can lead to the microphone icon displayed for an unrelated notification (CVE-2016-2829)
- A vulnerability when full-screen and pointerlock requests are done in combination with closing windows that could lead to denial of service attack or clickjacking. (CVE-2016-2831)
- An information-disclosure vulnerability in CSS pseudo-classes that can be used by web content to leak information on plugins that are installed but disabled. (CVE-2016-2832)
- A cross-site scripting vulnerability when the Content Security Policy (CSP) does not block loading of cross-domain Java applets when specified by policy (CVE-2016-2833)
- Network Security Services Vulnerabilities (CVE-2016-2834)

Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:
- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2016-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-52/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-53/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-54/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-55/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-56/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-57/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-58/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-59/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-60/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-61/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2815
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2818
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2819
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2822
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2824
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2825
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2826
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2828
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2829
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2831
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2832
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2833
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2834